Cyberwarfare experts explain the likely reasons for the lack of Russian cyberattacks so far

April 5 2022, by Nadiya Kostyuk and Erik Gartzke

Credit: Pixabay/CC0 Public Domain

Throughout the latter half of 2021, as it became clear that Russia was massing a large portion of its conventional combat power on the eastern borders of Ukraine, analysts offered contrasting predictions about the role cyberspace would play in an armed conflict. These predictions

capture an ongoing debate about whether conflict in cyberspace is destined to supplant conventional conflict or exacerbate it.

As the war has evolved, it's clear that analysts on both sides of the debate got it wrong. Cyber operations did not replace the military invasion, and as far as we can tell, the Russian government has not yet used cyber operations as an integral part of its military campaign.

We are political scientists who study the role of cybersecurity and information in international conflict. Our research shows that the reason pundits on both sides of the argument got it wrong is because they failed to consider that cyber and military operations serve different political objectives.

Cyber operations are most effective in pursuing informational goals, such as gathering intelligence, stealing technology or winning public opinion or diplomatic debates. In contrast, nations use military operations to occupy territory, capture resources, diminish an opponent's military capability and terrorize a population.

A tactical role for cyberattacks?

It's common in modern warfare for new technologies to substitute for traditional military tactics. For example, the U.S. has made extensive use of drones, including in conflicts in Yemen and Pakistan where crewed aircraft and ground forces would be difficult or impossible to use. Because drones allow the U.S. to fight on the cheap with much less risk, they substitute for other forms of warfare.

In theory, cyber operations could have played a similar tactical role in Russia's invasion of Ukraine. But the Russian government has yet to use cyber operations in a manner that is clearly coordinated with military units and designed to smooth the advance of ground or air forces. When

Russia invaded Ukraine, hackers disrupted access to satellite communications for thousands of people, and it was apparently a concern for Ukrainian defense officials. But overall, Ukraine has managed to maintain internet access and cellphone service for most of the country.

Russia has sophisticated cyber capabilities, and its hackers have worked their way into Ukrainian networks for many years. This raises the question of why Russia has not, for the most part, used cyber operations to provide tactical support for its military campaigns in Ukraine, at least until this point.

Separate roles

In recent studies, we examined whether cyber operations mostly serve as complements to, or substitutes for, conventional conflict. In one analysis, we examined conventional military campaigns around the world over a 10-year period using the Militarized Interstate Disputes dataset of all armed conflicts. We also focused on the conflicts in Syria and eastern Ukraine. Our results suggest that cyber operations are generally not being used as either.

Instead, nations tend to use these two types of operations independently from each other because each mode of conflict serves different objectives, and cyberwarfare is most effective for gathering intelligence, stealing technology or winning public opinion or diplomatic debates.

In contrast, nations use traditional forms of conflict to control tangible assets, such as capturing resources or occupying territory. The various goals offered by Russian President Vladimir Putin for invading Ukraine, such as preventing Ukraine from joining NATO, replacing the government or countering fictitious Ukrainian weapons of mass destruction, require occupying territory.

There may be other reasons for the lack of overlap between cyber and conventional fronts in Ukraine. The Russian military could consider cyber operations ineffective for its purposes. The newness of cyber operations as a tool of war makes it difficult to coordinate with conventional military operations. Also, military targets might not be accessible to hackers because they might lack internet connectivity.

In any event, evidence that the Russian government intends to use cyber operations to complement military operations is thin. Our findings suggest hacking groups in previous conflicts faced considerable difficulties in responding to battlefield events, much less shaping them.

How Russia is using cyber operations

The main target of Russia's digital campaign in Ukraine is ordinary Ukrainians. To date, Russian cyber operations have sought to sow panic and fear, destabilizing the country from within, by demonstrating the country's inability to defend its infrastructure, for example, by defacing or disabling websites.

In addition, Russia has been using information campaigns to attempt to win the "hearts and minds" of Ukrainians. Prior to the start of the conflict, White House press secretary Jen Psaki warned of a 2,000% increase from the daily average in November in Russian-language social media content. This suggests that the purpose of these information operations was to make the case for Russia's intervention on humanitarian grounds and to build support for intervention among the Ukrainian public. The Russian government's domestic actions emphasize the value its leadership places on information operations.

A supporting role

Hackers' actions tend to occur out of the public eye, rather than in the flamboyantly violent manner favored by Hollywood cyber villains, which means it's difficult to know for sure what's happening. Nevertheless, the lack of overlap between cyber and conventional military operations makes sense operationally and strategically. This is not to say that the informational focus of cyber operations has no effect on military operations. Good intelligence is essential for success in any military conflict.

We believe Russia is likely to continue conducting information campaigns to influence Ukrainians, its domestic public and international audiences. Russia is also likely to seek to further penetrate Ukrainian networks to access information that potentially assists its military operations. But because cyber operations have not been thoroughly integrated into its military campaigns so far, cyber operations are likely to continue playing a secondary role in the conflict.

Provided by The Conversation